RECEIVED
CENTRAL FAX CENTER
SEP 0 5 2006

REMARKS

The following remarks are made in response to the Non-Final Office Action mailed June 5, 2006. Claims 1-13, 16-22, 24, 26-35, 37 and 39-43 were rejected. Claims 14-15, 23, 25, 36, and 38 have been objected to. With this Response, claim 1 has been amended. Claims 1-43 remain pending in the application and are presented for reconsideration and allowance.

Claim Rejections under 35 U.S.C. § 112

The Examiner rejected claims 1-8 under 35 U.S.C. § 112, second paragraph, because the term "substantially similar" is a relative term, which renders the claim indefinite.

Amended independent claim 1 now recites, "to provide a second plaintext binary data sequence identical to the first plaintext binary sequence." As clarified, amended independent claim 1 is believed to be in allowable form. Dependent claims 2-8 depend from amended independent claim 1.

In view of the above, claims 1-8 are believed to be in form for allowance. Therefore, Applicant respectfully requests that rejections to these claims under 35 U.S.C. § 112, second paragraph, be reconsidered, and that the rejection be removed and these claims be allowed.

Claim Rejections under 35 U.S.C. § 102

The Examiner rejected claims 1-4, 7-13, 16-22, 24, 26-35, 37, and 39-43 under 35 U.S.C. § 102(e) as being anticipated by the Coppersmith et al. U.S. Patent No. 6,185,679.

Independent claims 1, 9, 18, and 31 all include limitations related to providing a keystream and cryptographically combining a first binary data sequence and the keystream and performing two sequential non-associative operations on the first binary data sequence and the keystream to provide the second binary data sequence. Independent claim 1 includes both an encryption combiner and a decryption combiner in a stream cipher cryptosystem. Independent claim 9 includes a cryptographic combiner (which could be an encryption combiner as claimed in dependent claim 10 or a decryption combiner as claimed in dependent claim 11) in a stream cipher cryptosystem. Independent claim 18 claims a method of encrypting a plaintext binary

data sequence. Independent claim 31 claims a method of decrypting a ciphertext binary data sequence.

Thus, independent claims 1, 9, 18, and 31 are include limitations related to stream cipher cryptosystems and methods. By contrast, the Coppersmith et al. patent discloses a method and apparatus for a symmetric block cipher cryptosystem.

Similar to as disclosed in the Background of the present specification, the Coppersmith et al. patent at column 2, beginning at line 6, discloses that encryption systems fall into two general categories. Symmetric (or secret key) (also referred to as private-key) encryption systems which use the same secret key for both encrypting and decrypting messages. The second general category is asymmetric (or public key) encryption systems which use different keys that are not feasibly derivable from one another for encryption and decryption. A person wishing to receive messages generates a pair of corresponding encryption and decryption keys. The encryption key is made public, while the corresponding decryption key is kept secret. The Coppersmith et al. patent further states at column 2, lines 26-29 that "the category of symmetric encryption systems can be further subdivided into those which operate on fixed sized blocks of data (block ciphers), and those which operate on arbitrary length streams of data (stream ciphers)." The Coppersmith et al. patent discloses a symmetric block cipher cryptosystem. In contrast, independent claims 1, 9, 18, and 31 claim stream cipher cryptosystems and methods.

Similar to as disclosed in Coppersmith et al., the Background section of the present specification discloses, beginning at page 1, line 30, that private-key (or symmetric key) cryptosystems are typically implemented as block cipher cryptosystems or stream cipher cryptosystems, where block cipher cryptosystems divide the plaintext into blocks and encipher each block independently using a stateless transform. In block cipher cryptosystems, if one fixed common private-key is employed to encipher different occurrences of a particular plaintext block, all of these occurrences are encrypted into identical corresponding ciphertext blocks. Therefore, the block size is preferably selected to be large enough to frustrate attacks from a cryptanalyst, which analyzes the occurrence frequencies of various patterns among the ciphertext blocks. By contrast, in stream cipher cryptosystems, the plaintext is typically encrypted on a bit-by-bit or word-by-word basis using a stateful transform that evolves as the encryption

progresses. In encrypting the plaintext binary data sequence for transmission as a ciphertext binary data sequence, the common private-key is a parameter that typically controls a pseudo-random number generator to create a long sequence of binary data referred to as a keystream. The stream cipher cryptosystem includes a cryptographic combiner, which combines the keystream with the plaintext sequence. The cryptographic combiner produces the ciphertext. At the receiver, the common private-key controls a receiver pseudo-random number generator to produce a decryption keystream. The decryption keystream is combined with a decryption combiner to decrypt the ciphertext to provide the plaintext to the receiver. One problem with a stream cipher cryptosystem is the difficulty of generating a long, statistically uniform, and unpredictable sequence of binary data in the keystream from a short and random key.

As acknowledged in both the Coppersmith et al. patent and the present specification, the problems, components, and solutions of symmetric block cipher cryptosystems, such as claimed and disclosed in the Coppersmith et al. patent, and the stream cipher cryptosystems and methods claimed in independent claims 1, 9, 18, and 31 are completely distinct.

In view of the above, the Coppersmith et al. patent does not teach or suggest the stream cipher cryptosystem of amended independent claim 1, the stream cipher cryptosystem of independent claim 9, the method of encrypting a plaintext binary data sequence of independent claim 18 or the method of decrypting a cipher text binary data sequence of independent claim 31.

In addition, dependent claims 1-4 and 7-8 further define patentably distinct amended independent claim 1; dependent claims 10-13 and 16-17 further define patentably distinct independent claim 9; dependent claims 19-22, 24, and 26-30 further define patentably distinct independent claim 18 and dependent claims 32-35, 37, and 39-43 further define patentably distinct independent claim 31. Therefore, these dependent claims are also believed to be allowable.

Therefore, Applicant respectfully requests reconsideration and withdrawal of the 35 U.S.C. § 102(e) rejection to claims 1-4, 7-13, 16-22, 24, 26-35, 37, and 39-43, and requests allowance of these claims.

Allowable Subject Matter

The Examiner objected to claims 14-15, 23, 25, 36, and 38 for being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all limitations of the base claim and any intervening claims.

Applicant respectfully points out that dependent claims 5 and 6 similar to provisionally allowed claims 14, 15, 23, 25, 36, and 38, claim features modular multiplication and inverse modular multiplication along with an XOR operation in a cryptographic combiner for performing two sequential non-associative operations on a first binary data sequence and a keystream to provide the second binary data sequence. Therefore, Applicant assumes in this Response that the Examiner intended to object to dependent claims 5 and 6 but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

Applicant agrees with the Examiner that dependent claims 5-6, 14-15, 23, 25, 36, and 38 would be allowable if rewritten in independent form. Nevertheless, as dependent claims 5-6 further define patentably distinct amended independent claim 1; dependent claims 14-15 further define patentably distinct independent claim 9; dependent claims 23 and 25 further define patentably distinct independent claim 18; and dependent claims 36 and 38 further define patentably distinct independent claim 31, these dependent claims are believed to be allowable in dependent form.

In view of the above, Applicant respectfully requests that the objections to dependent claims 5-6, 14-15, 23, 25, 36, and 38 be removed and that these claims be allowed.

CONCLUSION

In view of the above, Applicant respectfully submits that pending claims 1-43 are in form for allowance and are not taught or suggested by the cited references. Therefore, reconsideration and withdrawal of the rejections and allowance of claims 1-43 are respectfully requested.

No fees are required under 37 C.F.R. 1.16(b)(c). However, if such fees are required, the Patent Office is hereby authorized to charge Deposit Account No. 50-0471.

The Examiner is invited to contact the Applicant's representative at the below-listed telephone numbers to facilitate prosecution of this application.

Amendment and Response
Applicant: Kevin R. Driscoll
Serial No.: 09/712,505
Filed: November 14, 2000
Docket No.: H16-26353 (H162.104.101)
Title: CRYPTOGRAPHIC COMBINER USING TWO SEQUENTIAL NON-ASSOCIATIVE OPERATIONS

The Examiner is invited to contact the Applicant's representative at the below-listed telephone numbers to facilitate prosecution of this application.

Any inquiry regarding this Amendment and Response should be directed to either Patrick G. Billig at the below-listed telephone numbers or Kris T. Fredrick at Telephone No. (763) 954-5388. In addition, all correspondence should continue to be directed to the following address:

HONEYWELL INTERNATIONAL, INC.
Law Department AB2
P.O. Box 2245
Morristown, New Jersey 07962-9806

Respectfully submitted,

Kevin R. Driscoll,

By his attorneys,

DICKE, BILLIG & CZAJA, PLLC
Fifth Street Towers, Suite 2250
100 South Fifth Street
Minneapolis, MN 55402
Telephone: (612) 573-2003
Facsimile: (612) 573-2005

Date: 9-5-06
PGB:cmj:dmw

Patrick G. Billig
Reg. No. 38,080

CERTIFICATE UNDER 37 C.F.R. 1.8:

The undersigned hereby certifies that this paper or papers, as described herein, are being transmitted via facsimile to Facsimile No. (571) 273-8300 on this 5 day of September, 2006.

By:
Name: Patrick G. Billig